HHS' Updated Tracking Tech Guidance Offers Little Clarity

By **Wynter Deagle, Elfin Noce and Anne-Marie Dao** (March 27, 2024)

Wynter Deagle

Elfin Noce

Anne-Marie Dao

In an era dominated by digital interactions, the use of online tracking technologies has become ubiquitous. From cookies to pixels to web beacons, these tools allow organizations, including regulated entities, to collect and analyze user data, enhance user experience, personalize content and improve service delivery.

For entities regulated by the Health Insurance Portability and Accountability Act, however, the use of these technologies has involved walking a thin line between privacy and convenient access to care.

On March 18, the U.S. Department of Health and Human Services' Office for Civil Rights moved and further thinned that line by updating its controversial guidance on the use of online tracking technologies by HIPAA-covered entities and business associates.[1]

The December 2022 Guidance

In December 2022, the OCR issued a bulletin to provide guidance on the use of these technologies by HIPAA-regulated entities and, specifically, when the information collected by tracking technologies constituted individually identifiable health information, or IIHI, and therefore protected health information, or PHI, which is regulated by HIPAA.

The OCR's guidance was met with widespread criticism from the healthcare industry, including that it was overbroad and chilled covered entities' use of tracking technologies to reach patients in need or effectively provide general education resources to the public.

One of the main criticisms leveled against the 2022 bulletin was the OCR's guidance that the combination of an internet protocol address or any unique identifying code and health-related information is IIHI when it is collected by tracking technology on unauthenticated — i.e., publicly available and pre-login — webpages that address specific health conditions or healthcare providers.

This assertion was based on the OCR's apparent assumption that anyone visiting a covered healthcare provider's website was, is or will be a patient of the regulated entity. Specifically, the OCR concluded that all IIHI "collected on a regulated entity's website or mobile app generally is PHI, even if the individual does not have an existing relationship with the regulated entity."

In response, in November 2023, the American Hospital Association and certain Texas hospitals sued the OCR, seeking to bar enforcement of the portion of the guidance that restricts the use of tracking technologies that capture IP addresses on portions of healthcare providers' unauthenticated — public-facing and pre-login — webpages.

The lawsuit alleges that HHS exceeded its statutory authority by expanding the definition of

IIHI to include information collected "when an online technology connects (1) an individual's IP address with (2) a visit to an Unauthenticated Public Webpage that addresses specific health conditions or healthcare providers."[2]

It seeks to invalidate the portion of the guidance specific to unauthenticated webpages only. Following the filing of the AHA's opening brief in the case in January, 17 state hospital associations and 30 hospitals and health systems filed amicus briefs supportingthe AHA in the lawsuit.[3] The OCR is currently defending the lawsuit.

Changes in the Updated Guidance

Over a year after the 2022 bulletin was issued, and while the OCR is actively defending the AHA lawsuit, the OCR issued an updated the bulletin on the use of tracking technologies by regulated entities.

According to the text of the updated guidance, the 2022 bulletin was updated to "increase clarity for regulated entities and the public." While its position is somewhat clarified, the OCR's stance on the use of online tracking technologies has not softened.

Seemingly in response to the AHA lawsuit and amicus briefs, the OCR's updated guidance now acknowledges that
the mere fact that an online tracking technology connects the IP address of a user's device (or other identifying information) with a visit to a website addressing specific health conditions or listing health care providers is not a sufficient combination of information to constitute individually identifiable if the visit to the webpage is not related to an individual's past, present, or future health, health care, or payment for health care.

While this clarification puts the guidance in line with the statutory definition of IIHI, it does not make the application of the guidance by covered entities any easier.

Instead of adopting the bright-line rule endorsed by the AHA and numerous healthcare entities that information collected on unauthenticated webpages is not PHI, the updated guidance provides examples to "illustrate when certain visits to an unauthenticated webpage may or may not involve the disclosure of PHI."

Circumstances That May Involve Disclosure of PHI

The updated guidance provides two circumstances in which collection of information by a tracking technology from an unauthenticated webpage may involve disclosure of PHI because the information collected meets the definition of IIHI:

- When tracking technologies collect an individual's email address or reason for seeking healthccare — typed or selected from a drop-down menu — when a user visits an unauthenticated page and "makes an appointment with a health care provider or enters symptoms in an online tool to obtain a health analysis"; and

- When tracking technologies on a regulated entity's unauthenticated patient portal login page or registration page collect an individual's login information or registration information.

Circumstances That May Not Involve Disclosure of PHI

The updated guidance first explains that a user's visit to an authenticated webpages will not result in disclosure of PHI if the online tracking technologies on the webpages do not have access to information that relates to any individual's past, present or future health, healthcare or payment for healthcare.

The example provided for this category is when a website user "visits a hospital's webpage that provides information about the hospital's job postings or visiting hours."

Second, visits to unauthenticated webpages do not result in a disclosure of PHI if the visit is not related to an individual's past, present or future health, healthcare or payment for healthcare.

This category of visit hinges on the individual's motivation for visiting the website and OCR provides two examples to attempt to clarify of this category.

In the first example, a visit a webpage on the availability of oncology service by a student writing a term paper would not be considered PHI.

In the second example, the same visit to a listing of oncology services, but this time by an individual seeking a second opinion on treatment options, would be considered PHI "to the extent that the information is both identifiable and related to the individual's health or future health care."

Under these examples, the OCR appears to be suggesting that covered entities must be able to determine why an unauthenticated user is visiting a webpage to determine if PHI will be disclosed.

The updated guidance is silent, however, on how a covered entity is supposed to do this. The OCR's new approach provides little clarity to covered entities looking to comply with the updated guidance.

Covered entities are unlikely to have any knowledge of an individual's motivation for visiting their unauthenticated webpages. There can be a wide range of reasons an individual may visit a covered entity's webpage, including for healthcare services, review of a competitor's offerings or research for a family member.

Even with the two examples provided by the OCR, the webpage visitor could be by the same individual, with the only difference being the motivation for the visit.

A covered entity would have no way to discern that one visit was for a term paper and the other for a second opinion on treatment options. The updated guidance is silent on how a covered entity is supposed to discern a user's intent when using a public webpage. And, to date, no tracking technology collects motivation information.

Conclusion

As technology advances, so do the challenges of protecting PHI. Clear regulatory guidance is vital for covered entities struggling to understand and implement compliant tracking on their webpages.

The updated guidance, however, appears more focused on addressing the legal issues raised in the AHA litigation and less on practical guidance for covered entities. It is simply

impractical — if not impossible — for a covered entity to know the motivations of why individuals visit a public webpage.

Accordingly, covered entities should continue to carefully audit their current use and planned deployments of tracking technology, and incorporate assessments into their security risk analysis and management.

Wynter L. Deagle is a partner, and Elfin Noce and Anne-Marie Dao are associates at Sheppard Mullin Richter & Hampton LLP.

[1] https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html.

[2] https://www.aha.org/legal-documents/2023-11-02-case-complaint-aha-tha-thr-united-health-care-system-v-rainer.

[3] https://www.aha.org/news/headline/2024-03-19-ocr-updates-hipaa-guidance-use-online-tracking-technologies.